AMENDMENTS TO THE CLAIMS

Please amend claims 1 and 37 as shown in the listing of claims below. This Listing of Claims will replace all prior versions and listings of claims in the application. Added material is shown in underlined type, and deleted material is shown in ~~strikeout~~ type or within [[double brackets]]:

Listing of Claims

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A system for controlling use of requested digital content having usage rights associated therewith, said system comprising:

~~a server having digital content stored thereon;~~

a client computer having a standard application program including a standard rendering engine capable of being accessed to render content;

a communications network coupled to said client and said server; and

a client side security module, separate from the standard rendering engine, which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing ~~security conditions~~ usage rights for which the standard rendering engine is not operable to enforce and for providing access ~~accessing~~ to the standard rendering engine,

wherein, in response to a request to render the requested digital content, the security module determines [[if]] whether the requested digital content is protected content based upon the usage rights associated with the requested digital content, and

wherein, [[if]] when the requested digital content is protected content, the security module intercepts a request to the standard rendering engine to render the protected digital content, and

wherein, [[if]] when the security module determines that the requested digital content is protected content, the security module determines whether to allow a user to perform a requested function on the protected digital content based upon the

usage rights associated with the protected digital content, and responds to the request to perform the requested function on the protected digital content based on the usage rights associated with the protected digital content, and

wherein, [[if]] when the security module determines that the requested digital content is not protected content, the security module disengages from the standard rendering engine.

2-6. (Cancelled)

7. (Currently Amended) A system as recited in claim 1, wherein said security module is operative to define a user interface of said standard application program ~~in accordance with parameters specified by said server~~.

8. (Cancelled)

9. (Currently Amended) A system as recited in claim 1, wherein said security module is operative to superimpose a watermark based on client specific data on a image rendered by said standard rendering engine.

10. (Currently Amended) A system as recited in claim 9, wherein the client specific data is unique to the standard application program.

11. (Original) A system as recited in claim 9, wherein the client specific data is unique to the client computer.

12-19. (Cancelled)

20. (Currently Amended) A system as recited in claim 1, wherein said security module creates a document containing references to the digital content and

spawns a child instance of the standard rendering engine to render the document, and wherein said child instance of said standard rendering engine is operative to follow the references to retrieve content through an asynchronous protocol from a secured location.

21. (Original) A system as recited in claim 20, wherein said secured location is a trusted server system.

22. (Currently Amended) A system as recited in claim [[2]]1, wherein said standard rendering engine is a Web browser.

23. (Original) A system as recited in claim 1, further comprising a trusted server system and wherein said security module is operative to check security information of executable code to be loaded on said client computer to ascertain if said executable code is certified for security and if said executable code is certified, permitting said executable code to be installed on said client computer and wherein if said executable code is not certified, said server contacts said trusted site to verify if said executable code is certified by said trusted site and permits said executable code to be installed on said client computer if said executable code is authorized.

24-28. (Cancelled)

29. (Currently Amended) A system as recited in claim 1 [[28]], wherein said ~~document~~ digital content is an HTML document.

30-36. (Cancelled)

37. (Currently Amended) A method for controlling use of digital content having usage rights associated therewith, said method comprising:

~~storing digital content on a server;~~

requesting, over a communications network, the digital content from a client computer having a standard application program including a standard rendering engine capable of being accessed to render digital content; and

enforcing security conditions for accessing the standard rendering engine with a client side security module, separate from the standard rendering engine, which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing ~~security conditions~~ usage rights for which the standard rendering engine is not operable to enforce and for providing access to the standard rendering engine,

wherein, in response to a request to render digital content, said enforcing step comprises:

determining whether the requested digital content is protected content based upon the usage rights associated with the digital content;

~~selectively~~ intercepting a request to the standard rendering engine to render the protected digital content [[if]] when the client side security module determines that the requested digital content is protected content;

determining whether to allow a user to perform a requested function on the protected digital content based on the usage rights associated with the digital content [[if]] when the client side security module determines that the requested digital content is protected content;

responding to the request to allow a user to perform a requested function on the protected digital content based on the usage rights associated with the digital content [[if]] when the client side security module determines that the requested digital content is protected content; and

disengaging the client side security module from the standard rendering engine [[if]] when the client side security module determines that the requested content is not protected content.

38-42. (Cancelled)

43. (Currently Amended) A method as recited in claim 37, wherein said enforcing step comprises defining a user interface of said standard application program ~~in accordance with parameters specified by said server~~.

44. (Cancelled)

45. (Currently Amended) A method as recited in claim 37, wherein said enforcing step comprises creating a client specific watermark based on client specific data and superimposing the client specific watermark on a image rendered by said standard rendering engine.

46. (Currently Amended) A method as recited in claim 45, wherein the client specific data is unique to the standard application program.

47. (Original) A method as recited in claim 37, wherein the client specific data is unique to the client computer.

48-55. (Cancelled)

56. (Currently Amended) A method as recited in claim 37, wherein said enforcing step comprises creating a document containing references to the digital content and spawning a child instance of the standard rendering engine to render the document, and retrieving content through an asynchronous protocol from a secured location with said child instance of said standard rendering engine by following the references to.

57. (Currently Amended) A method as recited in claim 56, wherein said secured location is a trusted server ~~method~~ system.

58. (Currently Amended) A method as recited in claim 37 [[57]], wherein said standard rendering engine is a Web browser.

59. (Original) A method as recited in claim 37, wherein said enforcing step comprises checking security information of executable code to be loaded on said client computer to ascertain if said executable code is certified for security and if said executable code is certified, permitting said executable code to be installed on said client computer and wherein if said executable code is not certified, contacting a trusted site to verify if said executable code is authorized by said trusted site and permitting said executable code to be installed on said client computer if said executable code is authorized.

60-64. (Cancelled)

65. (Currently Amended) A method as recited in claim [[64]] 37, wherein said ~~document~~ digital content is an HTML document.

66-72. (Cancelled)

73. (Currently Amended) A system as recited in claim 1, further comprising:

an HTML document adapted to be rendered by Web browser in a secure environment, said document comprising:

an HTML header defined between header tags;

an HTML body containing content; and

security information embedded in said header, said security information being associated with one or more usage rights for the digital content,

wherein the HTML header, the HTML body, and the security information are delivered to a client computing system, and

the client computing system interprets the security information and honors the usage rights while processing the HTML body and the HTML header.

74. (Currently Amended) The system as recited in claim 73, wherein said HTML body does not contain security information for digital content in the HTML document.

75. (Currently Amended) The system as recited in claim 74, wherein said security information is in the form of an attribute of said HTML header.

76. (Previously Presented) A system as recited in claim 1, wherein the security module is installed on the client computer separately from the standard application program.

77. (Previously Presented) A system as recited in claim 1, wherein the security module is installed on the client computer at a different time than the standard application program.

78. (Previously Presented) A method as recited in claim 37, wherein the security module is installed on the client computer separately from the standard application program.

79. (Previously Presented) A method as recited in claim 37, wherein the security module is installed on the client computer at a different time than the standard application program.